



UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/755,452	01/05/2001	Scott C. Harris	FILE-DOMAIN/SCH	5147
23844	7590	08/26/2005	EXAMINER	
SCOTT C HARRIS P O BOX 927649 SAN DIEGO, CA 92192			TRAN, ELLEN C	
			ART UNIT	PAPER NUMBER

2134

DATE MAILED: 08/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/755,452

Applicant(s)

HARRIS, SCOTT C.

Examiner

Ellen C. Tran

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 27 May 2005.
- 2a) ☒ This action is FINAL. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-10, 12-16 and 18-27 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-10, 12-16, and 18-27 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: amendment filed on 27 May 2005, with original application filed 05 January 2001, and acknowledgement of continuing data filing date of 21 July 2000.
2. Claims 1-10, 12-16, and 18-27 are currently pending in this application. Claims 1, 10, 14, 22, and 23 are independent claims. Claims 3, 4, 12, 14, and 18, have been amended. Claims 11 and 17 have been cancelled.

Response to Arguments

3. Applicant's arguments with respect to claims 1-27 have been considered but have not been found persuasive.

In response to applicant's argument on page 8, *"However, according to Orita, the security is the security of a file, not the security of the user". Moreover, the files are each associated with security such as passwords, but the files are not associated with a user as claimed"*. The Office disagrees the files are associated with the user based on the user access level. In Orita the access level is used to associate the files with the user, this concept is not different than the claimed invention. In addition Orita describes storing an operator profile (OP), see col. 3, lines 1-9. The user profile includes user files this concept is well known.

In response to applicant's argument on page 8, *"However, nowhere is there any teaching or suggestion that a user can make changes to the first plurality of files that are associated with the user, but cannot read contents of the files when the user (with whom the files are associated) is not identified"*. The Office does not agree Orita shows this in col. 2, lines 4-7 "a program verifying unit for determining whether execution of the user program is permitted or not based

on the environment profile information read out from the second storage unit in response to starting request for the user program ... and an access verifying unit for determining whether execution of file access is permitted". It is obvious that if the program verifying unit cannot execute the files cannot be read, likewise if access to a file is not permitted the file cannot be read. Therefore Orita teaches a file cannot be read if the user ID/profile information does not pass verification or (when the user associated with the files are not identified).

In response to applicant's argument on page 9, *"Therefore, the files are not associated with specific users as defined by claim 1, but rather are associated with passwords and other kinds of "EP" information. As such, Orita does not describe "designating the first plurality of files in a computer as being associated with said user" as claimed"*. The Office disagrees Orita shows a user profile which has with it files associated with the user as col. 2, lines 4-7.

Furthermore files associated with a user are well known as user profiles.

In response to applicant's argument on page 9, *"While encryption per se is known, it is respectfully suggested that there is no teaching or suggestion of using encryption to prevent access to files that are not associated with the user, as claimed"*. The Office disagrees it is the combination, of encryption which is done to prevent unauthorized users from gaining access to files. The purpose of encryption is to prevent files from being accessed and protect data see '537 col. 1, lines 44-52 "To deter access to sensitive data and theft encryption algorithm have been employed to render the data unintelligible to unauthorized users".

In response to applicant's argument on page 9, *"nowhere is there any teaching or suggestion that the files are encrypted to "prevent reading content" and that a user who is associated with the files can read those files"*. The Office disagrees it is the combination, of

encryption which done to prevent unauthorized users from gaining access to files, i.e. access is interpreted to have the same meaning as “reading the contents”.

In response to applicant’s argument on page 10, *“Tello does teach a unique number, but it is used for identification of the computers, not for encryption”*. The Office disagrees Tello teaches the claimed invention as well as amended “wherein said ~~specified~~ unique information includes a unique number indicative of hardware in the computer system” in ‘537 col. 9, lines 20-31 and ‘537 col. 7, lines 63 through col. 8, line 26. The unique number identifies the smart card or IC the smart card contains the unique key or hash value which is used for encryption. “The flash memory of the security engine’s microprocessor contains six encryption algorithms. One algorithm is used for the generation of the hash number from the personalized information ... This algorithm is used to generate 3 hash numbers (H1, H2, H3) which are generated from the personal information inputted by the user ... These hash numbers are stored in the flash memory of the security engine microprocessor ... The third algorithm stored in the flash memory of the security engine microprocessor is used to generate a cryptographic key (CK) from H2’ ... This algorithm is the same as the one used by the smart card for all communications with the security engine”.

In response to applicant’s argument on pages 11-12, *“Finally, with all due respect, one having ordinary skill in the art would not make the hypothetical combination of Orita in view of Tello in the sway suggest by the Office Action ... Nowhere would there by any suggestion of encrypting files to restrain access, or the other features which have been described in detail above”*. The Office disagrees the purpose of encryption is to prevent files from being accessed and protect data see ‘537 col. 1, lines 44-52 “To deter access to sensitive data and theft

Art Unit: 2134

encryption algorithm have been employed to render the data unintelligible to unauthorized users". Therefore the combination of Orita and Tello is obvious.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. **Claims 1 and 9**, are rejected under 35 U.S.C. 102(e) as being anticipated by Orita U.S.

Patent No. 5,163,147 (hereinafter '147).

As to independent claim 1, **"A method, comprising: identifying a user using unique information; designating a first plurality files a computer as being associated with said user; responsive to said identifying"** is taught in '147 col. 1, line 57 through col. 2, line 19;

"using a program to said user to make a change to any of said first plurality of files associated said user" is shown in '147 col. 1, lines 40-42;

"and preventing reading contents of said first plurality files when said user is not identified" is disclosed in '147 col. 2, lines 4-7.

As to dependent claim 9, **"wherein preventing comprises preventing comprises preventing certain users from obtaining access to said files"** is taught in '147 col. 5, lines 55-63.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. **Claims 2-7, 10, 12-16, and 18-27** are rejected under 35 U.S.C. 103(a) as being unpatentable over ‘147 in further view of Tello U.S. Patent No. 6,463,537 (hereinafter ‘537).

As to dependent claim 2, the following is not taught in ‘147:

“wherein said preventing comprises encrypting files using an encryption value”

however ‘537 teaches “Modifications to the DDL and the inclusion of an I/O address map and circular memory buffer circuits also permit this invention to encrypt or decrypt selected data” in col. 19, lines 55-58.

“which requires said unique information form an encryption key” however ‘537 teaches “The level of access is determined by the presence or absence of encrypted keys in the memory of the security engine” in col. 5, lines 35-39.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of ‘147 a method for controlling access to files based on user access level to include a means utilize encryption mechanisms to protect selected files. One of ordinary skill in the art would have been motivated to perform such a modification to because as the use of computers increases the need to protect the information on the computers grows. As indicated

by '537 (see col. 1, lines 24 et seq.) "As the prevalence and importance of computers grows and their portability increases, so too does the need to protect these systems and the data stored within them from unauthorized access and theft".

As to dependent claim 3, "wherein said unique information includes a user password" is disclosed in '147 col. 3, line 10 "The user inputs ID information (incl. a password)".

As to dependent claim 4, "wherein said unique information includes a unique number indicative of hardware in the computer system" is taught in '537 col. 9, lines 20-25 "Written into the flash memory of the security engine microprocessor during its manufacture is also a secret identification number used in the identification of computers containing this invention over a network".

As to dependent claim 5, "further comprising designating a second plurality of files on the computer as read only" and "but not allowing any changes to said read only files" is shown in '147 col. 5, lines 1-7;

"and storing unencrypted information in said read files" is disclosed in '537 col. 19, lines 55-58 (Note: with modified motherboard a user can select which data to encrypt, therefore the data not selected is unencrypted).

As to dependent claim 6, "further comprising establishing a plurality of special files within said plurality of files, said special files being" and "and establishing special security measures for said special files" is taught in '147 col. 3, lines 1-21 "The read/write memory 14 includes an area 14a for storing operator profile (OP) information ... Access protection

information 12a (not shown) is included in each of the user programs 12e and each of the user files 12f”;

“said special files being unencrypted read/write files” is shown in ‘537 in col. 19, lines 55-58.

As to dependent claim 7, “wherein said security measures include determining whether a specified program actually accessing the file, and only allowing file access by said specified program” is disclosed in ‘147 col. 4, lines 49-60 “When an access request for a user file in the storage unit 12 is made by the user program (setp S11), permission of execution of the file access is verified”.

As to independent claim 10, “A method, comprising: storing both encrypted and unencrypted files on a computer” and “and storing encrypted information indicating results computer operations; taught in ‘537 col. 19, lines 55-58 “Modifications to the DDL and the inclusion of an I/O address map and circular memory buffer circuits also permit this invention to encrypt or decrypt selected data”;

“starting an operating system by reading said unencrypted files” is shown in ‘147 col. 2, lines 53 through col. 3, line 17;

“and designating unencrypted files as read only, and encrypted files as read/write files” is disclosed in ‘147 col. 5, lines 1-7.

As to dependent claim 12, “further comprising forming encrypted files by requiring a unique information, and using said unique as part of an encryption and/or decryption operation” is taught in ‘537 col. 5, lines 35-39.

As to dependent claim 13, **“further comprising establishing special files which are read/write files that are not encrypted, and carrying out least one security measure said special files”** is shown in ‘537 col. 19, lines 55-58.

As to independent claim 14, **“A computer, comprising: processor; a file accessing element, controlled by a controlling operation, said file accessing part controlling files in the computer in a way that prevents access specified files but allows access to other files unless specific unique information is used”** is shown in ‘147 col. 1, line 40 through col. 2, line 19;

“and wherein said file accessing part controls said access by encrypting said files” is disclosed in ‘537 col. 19, lines 45-58 **“The modified DDL also support the ability of the computer employing this invention to ‘hide’ restricted files or folders ...Modifications to the DDL and the inclusion of an I/O address map and circular memory buffer circuits also permit this invention to encrypt or decrypt selected data”**.

As to dependent claim 15, **“wherein said file accessing element allows access to all read files, and prevents access to read/write files”** is shown in ‘147 col. 1, lines 40-42;

“without said unique information” is disclosed in ‘147 col. 1, line 57 through col. 2, line 19.

As to dependent claim 16, **“wherein said file accessing element allows access to certain read write files which are designated as being special, is shown in ‘147 col. 1, lines 40-42;**

“and also conducts security check before allowing said access to said read write files” is disclosed in ‘147 col. 2, lines 4-7.

As to dependent claim 18, “wherein said encrypting comprises obtaining personal information from a user, and using said personal information to form encryption and/or decryption operations” is taught in ‘537 col. 5, lines 25-28.

As to dependent claim 19, “wherein said personal information a password” is shown in ‘147 col. 3, line 10.

As to dependent claim 20, “further comprising file storage part which includes removable memory” is disclosed in ‘537 col. 6, lines 15-37 “Peripheral data storage devices such as hard drive or DC ROM drive are connectd to the CPU via an IDE interface which is connected to the motherboard main Bus 108”;

“and wherein unencrypted read/write access is allowed to said removable memory” is shown in ‘537 col. 19, lines 55-58.

As to dependent claim 21, “wherein said file accessing element is part of an operating system” is taught in ‘147 col. 2, lines 53 through col. 3, line 17.

As to independent claim 22, “A method comprising: identifying using unique information; using an operating system associated program computer designate a first plurality of files a computer, as being associated with said user” is taught ‘147 col. 1, line 20 through col. 2, line 19.

“and to encrypt said plurality of files using an encryption system that includes said unique information” is shown in ‘537 col. 19, lines 55-58;

responsive to said identifying, using said operating system associated program in said computer to allow said user make any changes any of said first plurality files using said encryption system associated with said user and prevent reading contents said first

Art Unit: 2134

plurality of read/write files when said user not identified” is disclosed in ‘537 col. 15, lines 57-67

allowing other unencrypted files on said system be to be read when said user is not identified, but preventing writing to said other unencrypted files; and establishing special files on said system which are unencrypted but which can be written to and read by the system only after security operation and establishing special files on said system which are unencrypted but which can be written to and read by the system only after specified security operation” is taught in ‘147 col. 1, line 20 through col. 2, line 19.

As to independent claim 23, **“A method, comprising: obtaining a unique code from of the computer system; determining specified files on the computer system which qualify a specified security aspect”** is shown in ‘147 col. 1, line 20 through col. 2, line 19.

“and encrypting all other files other then said specified files said computer system, using said unique code” is disclosed in ‘537 col. 19, lines 55-58.

As to dependent claim 24, this claim contains substantially similar subject matter as claims 3 and is rejected along the same rationale.

As to dependent claim 25, **“wherein said unique code a code from a smart card”** is taught in ‘537 col. 5, lines 25-27 **“holder of a particular smart card”**.

As to dependent claim 26, **“wherein said unique code a code from a biometric”** is shown in ‘537 col. 7, lines 53-57 **“This allows for the addition of devices such as a biometric reader”**

As to dependent claim 27, **“wherein said unique code a code from a digital certificate”** is disclosed in ‘537 col. 5 lines 21 – 22 **“a unique has number (digital signature)”**.

8. **Claims 8** is rejected under 35 U.S.C. 103(a) as being unpatentable over '147 in further view of Porter et al. U.S. Patent No. 6,675,299 (hereinafter '299).

As to dependent claim 8, the following is not taught in '147: **“further comprising of accesses based on specified detecting certain kinds security criteria, and maintaining a log of said accesses including information about a program that made said accesses”** however '299 teaches “Finally, the document profile 710 contains the access history of the document. Access history includes information defining the user who created the document, and all users who accessed, modified, printed, or otherwise had contact with the document. The access history information includes the name of the user, the type of action performed by the user, and the time the user accessed the document” in '299 col. 8, lines 32-39.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '147 a method for controlling access to files based on user access level to include a management system, which maintains a history of file use. One of ordinary skill in the art would have been motivated to perform such a modification to because a management system is needed that maintains a log of access rights with an association to files. As indicated by '299 (see col. 2, lines 6-17.) “This two-step log-in procedure creates problems when the access rights are changed or when, for example, new users must be added to both security systems. Multiple sets of security information create configuration control and consistency problems ... Therefore, it is apparent that a need exists for a document management system which does not use a separate database and which does not utilize multiple security systems”.


Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Application/Control Number: 09/755,452
Art Unit: 2134

Page 14

Ellen. Tran
Patent Examiner
Technology Center 2134
19 August 2005